



CHAPTER 9

Dynamic Domain Name Server Updates

This chapter discusses DNS update methods and Server Address assignment, and provides configuration details of those features.

This chapter contains the following sections:

- [IP Reachability, page 9-1](#)
- [Configuring IP Reachability, page 9-2](#)
- [DNS Server Address Assignment, page 9-3](#)
 - [Support DNS Remapping on Home Agent, page 9-3](#)
- [Examples, page 9-4](#)

IP Reachability

TIA/EIA/IS-835-D describes dynamic DNS update method by the home AAA server and the Home Agent. DNS update by AAA is applicable to both Simple IP and Mobile IP service, while DNS update by the Home Agent is only applicable to Mobile IP service. The following describes the IP Reachability feature on Home Agent.

When the HA receives an initial Registration Request it sends a RADIUS Access-Request to the Home RADIUS server. If the RADIUS server is configured to request Home Agent-based DNS updates, the Home RADIUS server will include the DNS-Update-Required attribute in the RADIUS Access-Accept message returned to the HA. If the initial Mobile IP registration is successful, the HA sends a DNS Update message to the DNS server to add an A Resource Record for the MS. The HA sends a DNS Update message to the primary and secondary DNS server, if present.

When the HA receives a Mobile IP RRQ with lifetime timer set to zero, or the Mobile IP lifetime expires, or administrative operations invalidate the mobility binding for the MS, the Home Agent will send a DNS Update message to DNS server to delete the associated Resource Record. The following commands will enable the IP Reachability feature on Home Agent for the specified realm.



Note

DNS updates are not sent for each Re-registration.



Note

This feature is supported for Proxy Mobile IP flows as well.

The following call flow describes the IP Reachability on Home Agent - mobile registration scenario:

1. Home Agent receives a registration request from the PDSN/FA.
2. Home Agent sends an access request to RADIUS Server. The HA includes DNS Server Update Capability VSA.
3. The RADIUS server sends access accept with DNS Update Required VSA.
4. The HA sends Registration response to the PDSN/FA. If the HA is configured for redundancy, the active Home Agent will sync the binding creation to the standby Home Agent.
5. The HA creates a binding, and sends DNS Update request message to DNS Server
6. The DNS Server creates a DNS entry for the NAI, and sends DNS Update response message to the HA.

The following call flow describes the IP Reachability on Home Agent - Mobile deregistration scenario:

1. Home Agent receives a registration request with lifetime zero from PDSN/FA.
2. Home Agent sends an access request to RADIUS Server, if SA is not stored locally (optional).
3. RADIUS Server sends access accept (optional).
4. Home Agent deletes the binding. Home Agent sends Registration response to PDSN/FA. If Home Agent is configured for redundancy, the active Home Agent will sync the binding deletion to standby Home Agent.
5. Home Agent sends DNS Update request message to DNS Server, to delete the DNS entry.
6. DNS Server deletes the DNS entry for the NAI. DNS Server sends DNS Update response message to Home Agent.

Configuring IP Reachability

To enable this feature for the specified realm, issue the following commands:

	Command	Purpose
Step 1	Router(config)# ip name-server x.x.x.x	Specifies the address of one or more name servers to use for name and address resolution.
Step 2	Router(config)# ip mobile realm @ispxyz1.com dns dynamic-update method word	Enables the DNS Update procedure for the specified realm. <i>word</i> is the dynamic DNS update method name.
Step 1	Router(config)# ip mobile realm realm dns server primary dns server address secondary dns server address	Enables you to locally configure the DNS Server address.

To verify that this feature is enabled for a binding, use the following command:

	Command	Purpose
Step 1	Router# show ip mobile binding	Displays the mobility binding table.

The following example illustrates the realm configuration for IP reachability:

```
ip ddns update method sit-ha2-ddns2
  DDNS both
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
```

DNS Server Address Assignment

IS835D defines a method to push the home DNS server address to a mobile as an NVSE in a mobileip registration response. This procedure allows the Mobile Station to learn the primary and secondary DNS server address of its home domain.

The RADIUS server will include DNS Server VSA in an access response to the HA during mobile authentication. The HA forms a DNS server NVSE from the DNS Server VSA and adds it to mobileip registration response. If the DNS Server VSA is not received at the time of authentication, and DNS server address is configured locally on the Home Agent will form a DNS server NVSE from the local configuration and add it to mobileip registration response.

The DNS Server VSA and DNS Server NVSE carry primary and secondary DNS IP addresses.

DNS Server VSA will be synced to the standby if the HA is deployed in redundant mode.

To enable this feature for the specified realm, issue the following commands:

```
ip mobile realm realm dns server assign
ip name-server x.x.x.x
```

To locally configure the DNS Server address, issue the following command:

```
ip mobile realm realm dns server primary dns server address secondary dns server address
```

To verify that this feature is enabled for a binding, use the **show ip mobile binding** command.



Note

If the DNS server address is configured both locally and downloaded from AAA, then preference will be given to the local configuration on the HA.

Support DNS Remapping on Home Agent

In Cisco Mobile Wireless Home Agent Release 5.0, the Home Agent supports Stateful NAT capability with scaling to the number of subscribers supported by the Home Agent. This involves matching to a specific protocol and port so that DNS requests from a user can be recognized. Once recognized, the destination IP address is modified so that the DNS request is sent to the IP address defined by the operator. Similarly, the response has a source IP address of the DNS server that responded to the request. This is then mapped back to the original address used by the subscriber.

Examples

The following example illustrates how to configure a User profile for DNS:

```
[ //localhost/Radius/Profiles/mwts-mip-r20sit-haslb1-prof/Attributes ]
  CDMA-DNS-Server-IP-Address = 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
  CDMA-DNS-Update-Required = "HA does need to send DNS Update"
  CDMA-HA-IP-Addr = 20.20.225.1
  CDMA-MN-HA-Shared-Key = ciscociscociscoc
  CDMA-MN-HA-SPI = 00:00:10:01
  CDMA-Reverse-Tunnel-Spec = "Reverse tunneling is required"
  class = "Entering the World of Mobile IP-3"
  Service-Type = Framed
```

Here is a sample configuration of the DNS server address assignment realm:

```
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
```

The following example illustrates how to configure the same in AR user profile:

```
set CDMA-DNS-Server-IP-Address 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
```

The ones marked in **bold** text are primary and secondary DNS server address.

Here is a sample configuration of both IP Reachability and DNS Server Address Assignment:

```
ha2#show run
Building configuration...

Current configuration : 10649 bytes
!
! Last configuration change at 22:45:21 UTC Fri Nov 11 2005
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers
!
hostname tb1-6513-ha2
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa group server radius MOT
  server 150.2.0.1 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group MOT
aaa authorization config-commands
aaa authorization ipmobile default group MOT
aaa authorization network default group MOT
aaa authorization configuration default group MOT
aaa accounting session-duration ntp-adjusted
aaa accounting update newinfo periodic 3
aaa accounting network ha start-stop group MOT
aaa accounting system default start-stop group MOT
!
aaa server radius dynamic-author
```

```

client 150.2.0.1
server-key cisco
!
aaa session-id common
!
resource policy
!
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
ip dfp agent ipmobile
port 400
interval 15
inservice
!
ip ftp source-interface GigabitEthernet0/0.10
ip ftp username root
ip ftp password pdsnmwg
no ip domain lookup
ip name-server 10.77.155.10
ip name-server 1.1.1.1
ip name-server 6.6.6.6
no ip dhcp use vrf connected
no ip dhcp conflict logging
ip dhcp ping packets 0
!
ip dhcp pool Subnet-Pool1
utilization mark high 75
utilization mark low 25
origin dhcp subnet size initial /30 autogrow /30
!
!
ip vrf forwarding
!
ip vrf ispxyz
!
ip vrf ispxyz-vrf1
rd 100:1
!
ip vrf ispxyz-vrf2
rd 100:2
!
!
ip ddns update method sit-ha2-ddns1
DDNS both
!
ip ddns update method sit-ha2-ddns2
DDNS both
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group testsip1-l2tp
! Default L2TP VPDN group
! Default PPTP VPDN group
accept-dialin
protocol any
virtual-template 1
l2tp tunnel hello 0
!
username user-ha2 password 0 cisco
!

```

```

!
!
interface Tunnel10
  no ip address
  ip access-group 150 in
!
interface Loopback0
  ip address 20.20.225.1 255.255.255.0
!
interface Loopback1
  description address of the LNS server
  ip address 20.20.206.20 255.255.255.0
!
interface Loopback2
  ip address 170.12.0.102 255.255.0.0
!
interface GigabitEthernet0/0
  no ip address
  no ip route-cache cef
  no ip route-cache
  no keepalive
  no cdp enable
!
interface GigabitEthernet0/0.10
  description TFTP vlan
  encapsulation dot1Q 10
  ip address 10.77.155.5 255.255.255.192
  no ip route-cache
  no snmp trap link-status
  no cdp enable
!
interface GigabitEthernet0/0.172
  description HAAA interface
  encapsulation dot1Q 172
  ip address 170.2.0.20 255.255.0.0
  no ip route-cache
  no snmp trap link-status
  no cdp enable
  standby delay minimum 15 reload 15
  standby version 2
  standby 2 ip 170.2.0.102
  standby 2 follow sit-ha2
!
interface GigabitEthernet0/0.202
  description PI interface
  encapsulation dot1Q 202
  ip address 20.20.202.20 255.255.255.0
  no ip route-cache
  no snmp trap link-status
  no cdp enable
  standby delay minimum 15 reload 15
  standby version 2
  standby 2 ip 20.20.202.102
  standby 2 ip 20.20.204.2 secondary
  standby 2 ip 20.20.204.3 secondary
  standby 2 ip 20.20.204.4 secondary
  standby 2 ip 20.20.204.5 secondary
  standby 2 ip 20.20.204.6 secondary
  standby 2 timers msec 750 msec 2250
  standby 2 priority 130
  standby 2 preempt delay minimum 180
  standby 2 name sit-ha2
!
interface GigabitEthernet0/0.205

```

```

description REF interface
encapsulation dot1Q 205
ip address 20.20.205.20 255.255.255.0
no ip route-cache
no snmp trap link-status
no cdp enable
standby delay minimum 15 reload 15
standby version 2
standby 2 ip 20.20.205.102
standby 2 follow sit-ha2
!
interface Virtual-Templat1
description To be used by VPDN for PPP tunnel
ip unnumbered Loopback1
peer default ip address pool LNS-pool
no keepalive
ppp accm 0
ppp authentication chap pap optional
ppp accounting none
!
router mobile
!
ip local pool LNS-pool 7.0.0.1 7.0.0.255
ip local pool ispxyz-vrf1-pool 50.0.0.1 50.0.0.255
ip local pool mobilenodes 40.0.0.1 40.0.100.255
ip default-gateway 10.77.155.1
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0.202
ip route 10.77.139.29 255.255.255.255 10.77.155.1
ip route 150.2.0.0 255.255.0.0 170.2.0.1
no ip http server
!
!
ip mobile debug include username
ip mobile home-agent template Tunnel10 address 20.20.202.102
ip mobile home-agent revocation timeout 5 retransmit 4
ip mobile home-agent dynamic-address 20.20.202.102
ip mobile home-agent accounting ha broadcast lifetime 3600 replay 8 suppress-unreachable
unknown-ha deny
ip mobile home-agent redundancy sit-ha2 virtual-network address 20.20.202.102
periodic-sync
ip mobile radius disconnect
ip mobile virtual-network 50.0.0.0 255.0.0.0
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai mwts-pmp-r20sit-base-user1@ispxyz1.com virtual-network 40.0.0.0
255.0.0.0 aaa load-sa lifetime 600
ip mobile host nai @ispxyz2.com address pool local mobilenodes virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 180
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server 10.77.155.10 1.1.1.1
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server assign
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns dynamic-update method
sit-ha2-ddns1
ip mobile realm @ispxyz2.com vrf ispxyz-vrf2 ha-addr 20.20.204.6
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
ip mobile secure foreign-agent 20.20.201.10 20.20.201.100 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
ip mobile secure foreign-agent 20.20.210.10 20.20.210.100 spi 100 key ascii cisco replay
timestamp within 5 algorithm md5 mode prefix-suffix
ip mobile secure home-agent 20.20.202.10 20.20.202.95 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
!
ip radius source-interface Loopback2

```

```
no logging trap
logging source-interface GigabitEthernet0/0.201
access-list 150 permit ip host 40.0.0.1 host 20.20.205.220 log
access-list 150 permit ip host 20.20.205.220 host 40.0.0.1 log
access-list 150 deny ip any any log
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source Loopback0
snmp-server host 150.2.0.100 version 2c private
snmp-server host 150.2.0.100 public
no cdp run
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 55 access-request include
radius-server host 150.2.0.1 auth-port 1645 acct-port 1646 key 7 121A0C041104
radius-server host 150.2.0.100 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 4
radius-server timeout 2
radius-server deadtime 5
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
alias exec shc sh cdma pdsn
alias exec ua undebg all
alias exec ui undebg ip packet
!
line con 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
line vty 5 15
  exec-timeout 0 0
!
!
end

ha2#
```